



QUALYS SECURITY CONFERENCE 2018

Ignore APIs at Your Peril

Qualys and 42Crunch Partner to Deliver API Security

Jacques Declas
CEO, 42Crunch

Everyone loves containers

API Security Breaches are Mounting



“By 2022 API abuses will be the attack vector most responsible for data breaches within enterprise web applications”

Gartner Research - G342236

Why is securing APIs so difficult today?

Enterprise Perimeter is Disappearing

Proliferation of end points, internet facing APIs, virtual network, micro-services architecture, distributed security enforcement points

Lack of API Security Tools and Standards

No API Security standards, Complexity of API Security (Integrity, Confidentiality, AAA, non-repudiation..), no proven reusable API Security policies

Current Solutions Don't Work for API's

Web Application Security is not API Security, multiple solutions to cover part of API Security (CDN, WAF, API Gateway, Code...), API Developers often try to code Security into their APIs

Distributed, Unified, API Specific Security enforcement points

Web App Security

Traditional White list/Black,
hard to maintain, False positives

In-line WAF single layer
north-south only, DMZ only

Operational Model

Deployment

API Specific attacks

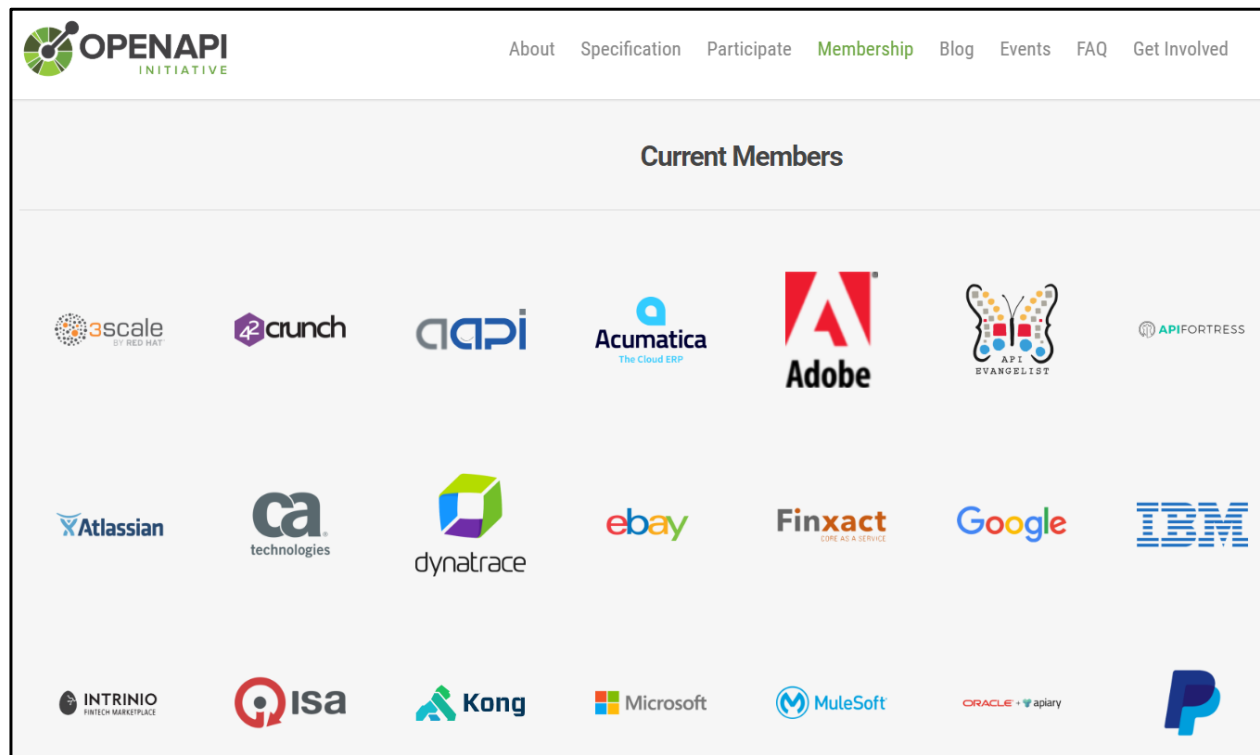
API request validation (OAS 2.0)
XML & JSON schema validation
XML Threat Protection.
JSON Threat Protection
JSON Path / JSON Pointer injections
SQL Injection Vulnerability detection in encrypted
OAuth Security ext. support PKCE, token binding
JOSE, draft-cavage-http-signatures
Cross-Site Scripting attack detection

API Security

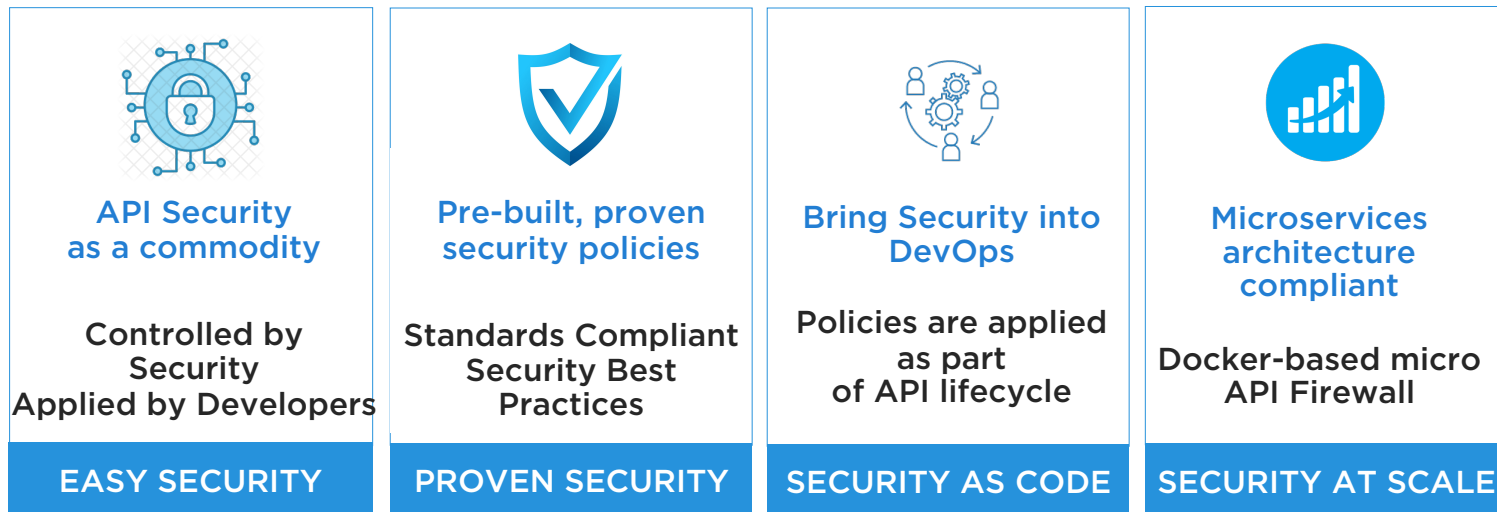
Positive automatic security
model, DevSecOps

Centralised or distributed.
Support Microservices,
Serverless, East-West, Sidecar

Developers Must use the Standard

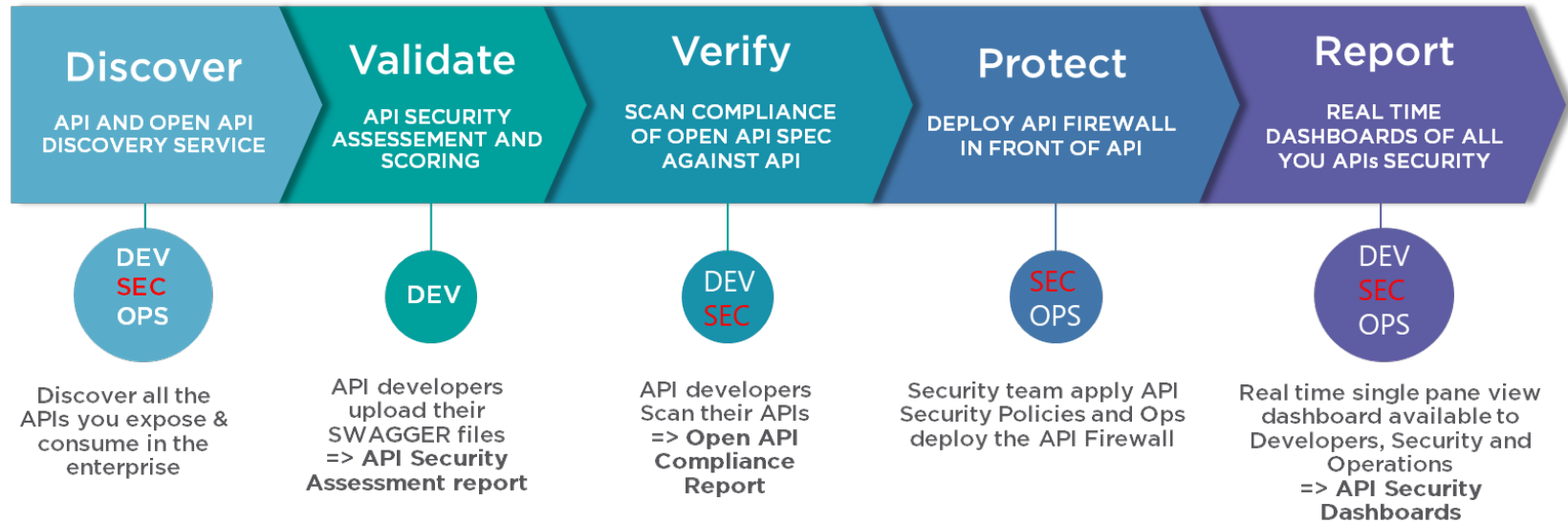


Changing the API Security Model



API Security

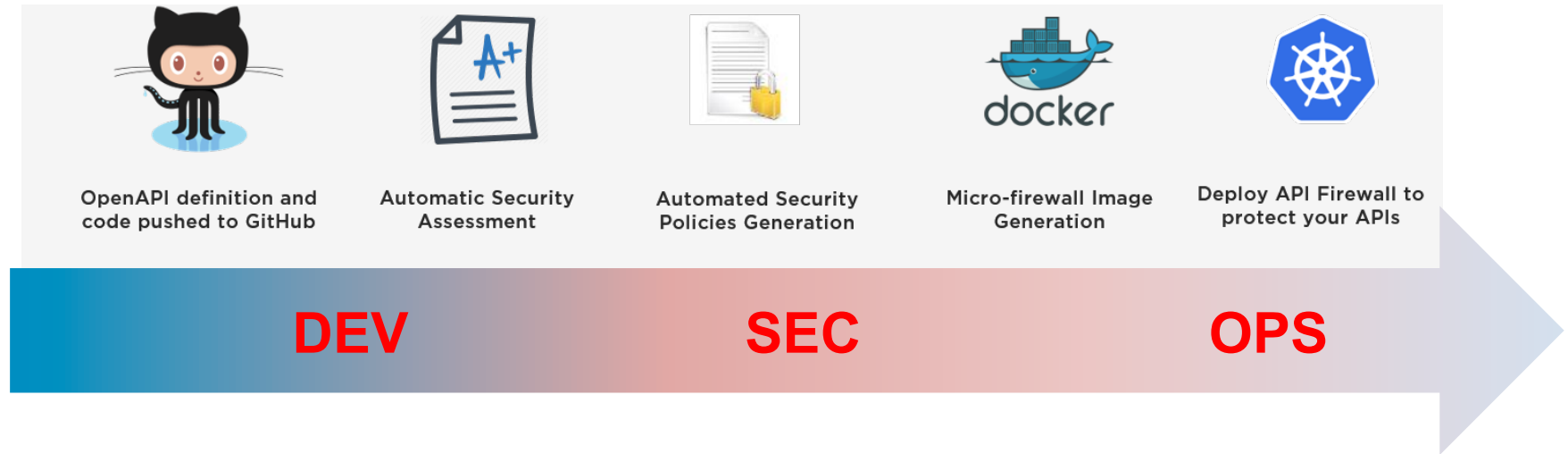
DevSecOps approach



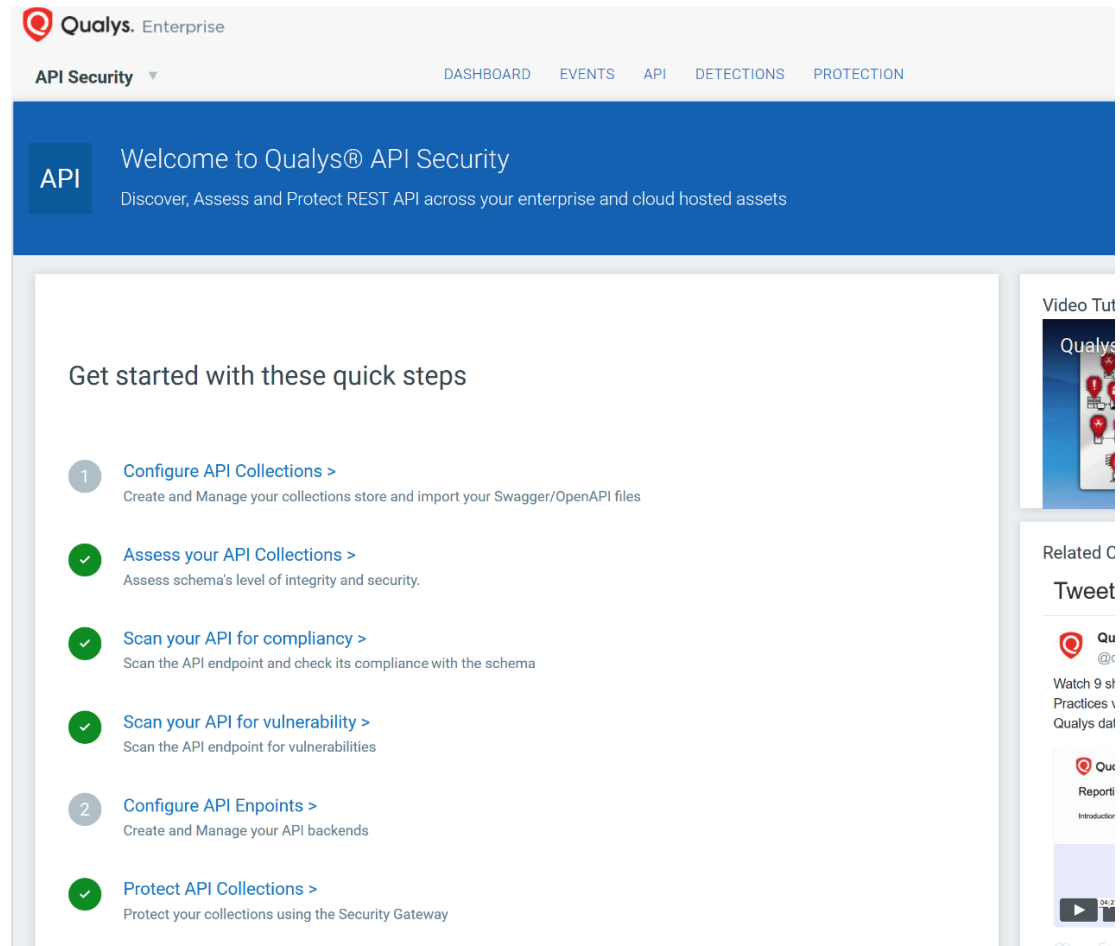
Prebuilt Security Policies and Packages

| Package Name | Transport Constraints | Request / Response Validation | Token Validation | Message Validation | Payload Crypto-Operations | Authentication | Authorization | Audit |
|--------------|------------------------------|--|---------------------------------|--------------------------|-------------------------------------|------------------------------------|---|---------------------------------|
| | TLS version and CipherSuites | Data Validation & OWASP Attacks Protection | OAuth/OpenID Attacks Protection | OWASP Attacks Protection | Message Confidentiality & Integrity | Identity Validation (Basic/OpenID) | Fine-grain Authorization (Scopes/XACML) | Audit Trail and Non Repudiation |
| OWASP | ✓ | ✓ | ✓ | ✓ | | | | ✓ |
| Open Banking | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| PCI-DSS | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 42C standard | ✓ | ✓ | | ✓ | | | | ✓ |

End to end API Security Process



End-to-End API Security Platform



Qualys. Enterprise

API Security ▾ DASHBOARD EVENTS API DETECTIONS PROTECTION

API Welcome to Qualys® API Security
Discover, Assess and Protect REST API across your enterprise and cloud hosted assets

Get started with these quick steps

- 1 [Configure API Collections >](#)
Create and Manage your collections store and import your Swagger/OpenAPI files
- ✓ [Assess your API Collections >](#)
Assess schema's level of integrity and security.
- ✓ [Scan your API for compliancy >](#)
Scan the API endpoint and check its compliance with the schema
- ✓ [Scan your API for vulnerability >](#)
Scan the API endpoint for vulnerabilities
- 2 [Configure API Endpoints >](#)
Create and Manage your API backends
- ✓ [Protect API Collections >](#)
Protect your collections using the Security Gateway

Video Tut
Qualys
Related C
Tweet
Qu
@c
Watch 9 st
Practices v
Qualys dal
Qu
Reporti
Introduction
Qu
@c



QUALYS SECURITY CONFERENCE 2018

Thank You

Jacques Declas
CEO, 42Crunch